Per an FSA personnel request, the Security and Privacy Team reviewed the security contract language for a new system and made recommendations on changes. They also sent the system a draft copy of the new security contracting language.

Security

Given the sensitive nature of student Privacy Act data supplied to the Department of Education, it will be necessary for the FEBI solution to demonstrate ample precautionary measures aimed at the protection of data. The FEBI security approach must conform to Federal Security Requirements and FSA Security Guidelines. Any FEBI systems implementation must include obtaining security certification and accreditation, as required of all ED systems. Moreover, since the FEBI solution does not contain explicit boundaries, the security of communications and other business systems is paramount. The FEBI solution should present the following practices and procedures in a detailed security plan that meets the required format proscribed in NIST 800-18:

Deleted: supplied to

Deleted: Standard ?:

- Access control and methodology (including intrusion detection and alerts)
- Identification and Authorization
- Application and systems development security
- Business continuity and disaster recovery planning. The FEBI solution will need to include an extremely comprehensive and demonstrated data recovery strategy that includes an annual disaster recovery exercise per federal regulations and guidance (Appendix E for what?). This strategy must support business resumption should any type of disaster occur and meet contractual standards for system availability and response time.

- Law, investigation and ethics
- Operations security
- Physical security
- Security architecture and models
- Security management practices
- Telecommunications and networking

A number of individuals will require access to the information contained in the system for a variety of reasons such as providing customer service, developing and testing new functionality, and analyzing data for portfolio management, querying the database for reporting and analysis, among others. These individuals must only be given access to the information deemed appropriate for their job responsibilities and level of security clearance.